Authentication of a Computer-Based System— Possible Authentication Methods Using the AMS/IB Computational Block as an Example

James Fuller
Pacific Northwest National Laboratory

The purpose of authentication is to give confidence to monitors that host-supplied or -certified equipment will make credible measurements. This means that the monitor needs confidence that (1) the system has been assembled as designed, (2) the system functions as designed, and (3) the system does not contain a "hidden-switch" that allows the host to pass out-of-specification materials.

The term "hidden switch" is used to denote any method, device, or feature in the measurement system that could be used by the host to fool the monitor. A hidden switch could enable the host to covertly and erroneously pass selected canisters. A hidden-switch could reside in either hardware or software, or in a combination of both.

There are basically three methods that can be used to authenticate an assembled measurement system with an integral information barrier: (1) the use of trusted, unclassified calibration sources; (2) the random selection of modular system elements; and (3) the availability and use of complete design documentation. The use of trusted, unclassified calibration sources was the subject of another hands-on presentation at the August demonstration. Ideas on how methods (2) and (3) might be utilized will be considered below in relation to the AMS/IB computational block.

The actual implementation of these methods will be enhanced if the authentication requirement is a factor considered as a part of the design process. System elements that support the concept of easy inspection should be selected. Where possible, elements that perform the same or a very similar function should be selected so that they are themselves identical.

The computational block is one of five central processing modules used in the AMS/IB. Its function is to receive the data from the detector subsystems, compute whether or not the inspected item meets the attribute conditions expected, and to trigger the proper 1-bit result (yes/no) answer for each attribute. A good design package will include functional specifications, as-built annotated photographs, and listing of major hardware and software elements. This information was presented for the computational block as part of the August 2000 Los Alamos AMS/IB demonstration.

The concept of random selection of elements and subsystems involves the host procuring multiple identical copies of this hardware and software which are to be made available to the monitor for selection at appropriate times, according to specific procedures previously agreed to by both parties. Random selection by a monitor between two pieces of new (never used) identical hardware or software, wherein one piece is chosen for installation in the measurement system and the other becomes the possession of the monitor to take

home for private examination, is a very powerful confidence-building tool. Such a process will provide a monitor with the maximum confidence in the integrity of the system. An example of computational block modules that might be suited for random selection include the whole, fairly compact, block itself, the CPU motherboard, or the PROM integrated circuit holding the operational software.

The use of documentation to authenticate complex hardware and software is limited by the complexity of this equipment. This is one reason it is very important to utilize systems that are only as complex as they absolutely need to be (systems that have had extraneous functionality removed). Also, the right of the monitor to randomly select for focused inspection any subsystem of a complex integrated measurement system can be a very effective authentication tool. The usefulness of detailed documentation for authentication is maximized if the integrated measurement system has been jointly developed. The usefulness of hard-copy source code documentation of software for authentication is limited, especially for complex code. The availability of machine-readable source code expedites authentication. Methods and procedures to validate source code and compiled code would be a very good subject for joint study. As part of the demonstration, examples of other documentation were provided, including detailed schematics, complete parts lists, mechanical dimensions and configurations of printed circuits, jumper and connector maps and listings for all printed circuits, software initialization parameters and values, and complete integrated circuit memory maps. There are limited possibilities available to authenticate PROM software; the solution to this would be an excellent subject for joint development.